Universita' degli Studi di Roma "Tor Vergata"
Laurea Triennale in Matematica - a.a. 2024/2025
Corso: Algebra 1
Docente: Prof.ssa I. Damiani, Codocente: Prof. F. Flamini

Esercitazioni/Tutorati 12-13 (26-27 Maggio 2025) - Prof. F. Flamini

Esercizio 1. Sia $\mathbb{Z}[i]$ l'**anello degli interi di Gauss**

(i) Dopo aver ricordato che $\mathbb{Z}[i]$ é **dominio euclideo**, dati $\alpha := 14-3i,\ \beta := 4+7i \in \mathbb{Z}[i]$, determinare MCD$(\alpha,\ \beta)$ e descrivere un'identità di Bezout per esso.

(ii) Dimostrare che l'ideale $I := (3) \subset \mathbb{Z}[i]$ é primo (equiv. massimale); dedurre che l'anello quoziente $\frac{\mathbb{Z}[i]}{I}$ é un campo $\mathbb{K}$ e se ne determini la cardinalitá e l'inverso in $\mathbb{K}$ dell'elemento $[2+i] := 2+i+I \in \mathbb{K}$.

(iii) Dimostrare che il campo $\mathbb{K}$ determinato al punto (ii) é isomorfo al campo $\mathbb{H} := \frac{(\mathbb{Z}/3\mathbb{Z})[x]}{(x^2+\overline{1})}$, con $x^2+\overline{1}$ polinomio irriducibile nell'anello euclideo $(\mathbb{Z}/3\mathbb{Z})[x]$.

(iv) Dato $a+bi := 3+i \in \mathbb{Z}[i]$, utilizzando che MCD$(a,b)$ = MCD$(3,1) = 1$ in $\mathbb{Z}$, stabilire che l'anello quoziente $\frac{\mathbb{Z}[i]}{(3+i)}$ é isomorfo all'anello quoziente $\mathbb{Z}/10\mathbb{Z}$, e dunque non é un dominio di integritá

(v) Dedurre che la procedura utilizzata per risolvere il punto (iv) si estende piú generalmente al seguente enunciato:
Dato $a+bi \in \mathbb{Z}[i]$ con MCD$(a,b) = 1$ *in $\mathbb{Z}$, i.e. a e b interi* **coprimi**, *l'anello quoziente $\frac{\mathbb{Z}[i]}{(a+ib)}$ é isomorfo all'anello quoziente $\mathbb{Z}/(a^2+b^2)\mathbb{Z}$, e pertanto é un campo se e solo se la* **valutazione** *dell'elemento $a+bi \in \mathbb{Z}[i]$ é un numero primo $p \in \mathbb{N}$.*

Esercizio 2. Si consideri il dominio euclideo $\mathbb{Z}$.
(i) Consideriamo $\mathbb{Z}[\frac{1}{2}] \subset \mathbb{Q}$ il minimo sottoanello di $\mathbb{Q}$ che contenga $\mathbb{Z}$ e $\{\frac{1}{2}\}$. Verificare che $\mathbb{Z}[\frac{1}{2}]$ é un **dominio euclideo**. Dedurre infine che **si arriva alla stessa conclusione** se si sostituisce 2 con un qualsiasi $a \in \mathbb{Z} \setminus \{0\}$ e si considera l'anello $\mathbb{Z}[\frac{1}{a}] \subset \mathbb{Q}$ (ritrovando $\mathbb{Z}$ se e solo se $a = \pm 1$).

(ii) Consideriamo $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ il minimo sottoanello di $\mathbb{R}$ che contenga $\mathbb{Z}$ e $\{\sqrt{2}\}$. Verificare che $\mathbb{Z}[\sqrt{2}]$ é un **dominio euclideo**. Osservare che, a differenza del caso (i), **non si arriva alla stessa conclusione** se si sostituisce 2 con un qualsiasi $a \in \mathbb{N} \setminus \{0\}$ e si considera l'anello $\mathbb{Z}[\sqrt{a}] \subset \mathbb{R}$, verificando ad esempio che $\mathbb{Z}[\sqrt{10}]$ non é **DFU** (quindi non puó essere euclideo) dimostrando che $10 \in \mathbb{Z}[\sqrt{10}]$ ha due fattorizzazioni non banali distinte in irriducibili.

(iii) Consideriamo $\mathbb{Z}[\sqrt{-2}] \subset \mathbb{C}$ il minimo sottoanello di $\mathbb{C}$ che contenga $\mathbb{Z}$ e l'insieme $\{\sqrt{-2} = i\sqrt{2}\}$. Verificare che $\mathbb{Z}[\sqrt{-2}]$ é un **dominio euclideo**. Osservare che, a differenza del caso (i), **non si arriva alla stessa conclusione** se si sostituisce 2 con un qualsiasi $a \in \mathbb{N} \setminus \{0\}$ e si considera l'anello $\mathbb{Z}[\sqrt{-a}] \subset \mathbb{C}$, verificando ad esempio che $\mathbb{Z}[\sqrt{-3}]$ non é **DFU** (quindi non puó essere euclideo) dimostrando che $1+\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ é un elemento **irriducibile** ma **non primo**.

Esercizio 3. Anello delle serie formali: $\mathbb{K}[[x]]$ é l'insieme delle serie formali in x a coefficienti in $\mathbb{K}$, i cui elementi sono espressioni della forma

$$\underline{a} := \sum_{n\geq 0} a_n x^n,\ a_n \in \mathbb{K}$$

(i) Descrizione delle operazioni di anello $+$ e $\cdot$ che lo rendono **anello commutativo unitario**

(ii) Definizione di **grado**, per ogni $\underline{a} \in \mathbb{K}[[x]] \setminus \{\underline{0}\}$ come

$$\deg(\underline{a}) := \min_{n\in\mathbb{N}}\{a_n \neq 0 \text{ in } \underline{a}\}$$

che lo rende **dominio di integritá**.

(iii) Caratterizzazione degli invertibili in $\mathbb{K}[[x]]$:
$\underline{a} \in U(\mathbb{K}[[x]])$ se e solo se $a_0 \neq 0$, i.e. se e solo se $\deg(\underline{a}) = 0$.

(iv) Caratterizzazione degli ideali in $\mathbb{K}[[x]]$:
tutti e soli gli ideali propri di $\mathbb{K}[[x]]$ sono della forma (x^n), per $n \geq 1$, pertanto $\mathbb{K}[[x]]$ é **PID**, gli ideali formano una **catena ascendente** di inclusioni proprie

$$\cdots \subset (x^{n+1}) \subset (x^n) \subset \cdots \subset (x^2) \subset (x) \subset \mathbb{K}[[x]],$$

e dunque $\mathbb{K}[[x]]$ ha come unico **ideale massimale=massimo** l'ideale (x).

(iv) Per ogni $n \geq 1$, dimostrare che si ha l'isomorfismo d'anelli

$$\frac{\mathbb{K}[[x]]}{(x^n)} \cong \frac{\mathbb{K}[x]}{(x^n)},$$

dove $\mathbb{K}[x]$ l'usuale dominio euclideo dei polinomi a coefficienti in $\mathbb{K}$ nell'indeterminata x.

(vi) Determinare il **campo dei quozienti** $\mathbb{K}((x)) := \mathcal{Q}(\mathbb{K}[[x]])$ del dominio integro $\mathbb{K}[[x]]$ detto **campo delle serie di Laurant**. Osservare che, dalla naturale inclusione di domini integri $\mathbb{K}[x] \subset \mathbb{K}[[x]]$, si deduce una inclusione di campi $\mathbb{K}(x) \subset \mathbb{K}((x))$, dove $\mathbb{K}(x) = \mathcal{Q}(\mathbb{K}[x])$ é il **campo delle funzioni razionali** in x a coefficienti in $\mathbb{K}$.

(vii) Dimostrare $\mathbb{K}[[x]]$ é un **dominio euclideo**.

Esercizio 4. Si consideri il polinomio $f(x, y) \in \mathbb{R}[x, y]$ dato da

$$f(x, y) = y^3 - (x^2 + 1).$$

Un punto $P = (x_0, y_0) \in \mathbb{R}^2 = \mathbb{A}^2(\mathbb{R})$ si dice **soluzione** di $f(x, y)$ se $f(x_0, y_0) = 0$, i.e. se vale

$$y_0^3 = x_0^2 + 1,$$

equivalentemente $P = (x_0, y_0) \in C$ dove C la **curva affine** determinata da

$$C := \{P = (x_0, y_0) \in \mathbb{R}^2 = \mathbb{A}^2(\mathbb{R}) \,|\, y_0^3 = x_0^2 + 1\}.$$

(i) Stabilire che se (x_0, y_0) é **soluzione intera** di $f(x, y)$, i.e. $(x_0, y_0) \in \mathbb{Z} \times Z$ (equivalentemente P su C é un **punto a coordinate intere**) allora $x_0 \in \mathbb{Z}$ é necessariamente un numero intero pari.

(ii) Se (x_0, y_0) é soluzione intera di $f(x, y)$, stabilire che gli elementi $x_0 + i,\ x_0 - i \in \mathbb{Z}[i]$ sono **coprimi** nell'anello degli interi di Gauss $\mathbb{Z}[i]$.

(iii) Dedurre da (ii) e dal fatto che (x_0, y_0) é soluzione intera di $f(x, y)$, che allora gli elementi $x_0+i,\ x_0-i \in \mathbb{Z}[i]$ sono **cubi** in $\mathbb{Z}[i]$, i.e. esistono $\alpha := a+ib, \beta := a'+ib' \in \mathbb{Z}[i]$ tale che $x_0 + i = \alpha^3$, $x_0 - i = \beta^3$.

(iv) Dedurre da (iii) che $f(x, y)$ ha come unica soluzione intera $(x_0, y_0) = (0, 1)$ (equivalentemente l'unico punto P a coordinate intere su C é $P = (0, 1)$).

Esercizio 5. (i) Si consideri il dominio euclideo $(\mathbb{Z}, +, \cdot)$ e l'anello **prodotto diretto** $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ con

$$(m, n) + (m', n') := (m + m', n + n') \text{ e } (m, n) \cdot (m' + n') := (m \cdot m', n \cdot n').$$

Dopo aver verificato che $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ é commutativo, unitario ma non é dominio di integritá, determinare (a meno di isomorfismo) la struttura del **gruppo degli automorfismi di anello** (i.e. omomorfismi dell'anello $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ in sé che sono iniettivi e suirettivi)

$$(Aut(\mathbb{Z} \times \mathbb{Z}, +, \cdot), \circ),$$

dove l'operazione di gruppo $\circ$ é la composizione di automorfismi.

(ii) Si consideri il gruppo abeliano ciclico $(\mathbb{Z}, +)$ ed il gruppo additivo **prodotto diretto** $(\mathbb{Z} \times \mathbb{Z}, +)$ con

$$(m, n) + (m', n') := (m + m', n + n').$$

Dopo aver verificato che $(\mathbb{Z} \times \mathbb{Z}, +)$ é abeliano, determinare (a meno di isomorfismo) la struttura del **gruppo degli automorfismi di gruppo** (i.e. omomorfismi del gruppo abeliano $(\mathbb{Z} \times \mathbb{Z}, +)$ in sé che sono iniettivi e suirettivi)

$$(Aut(\mathbb{Z} \times \mathbb{Z}, +), \circ),$$

dove l'operazione di gruppo $\circ$ é la composizione di automorfismi.

Esercizio 6. Per i seguenti gruppi sotto elencati, determinare la loro cardinalitá, stabilire se sono gruppi ciclici o meno, ed in caso di risposta affermativa determinare tutti i loro generatori, descrivere tutti i loro sottogruppi stabilendo se essi sono ciclici o meno, determinare infine la struttura (a meno di isomorfismi) del gruppo dato e di tutti i suoi sottogruppi.

(i) $U(\mathbb{Z}/8\mathbb{Z})$= gruppo moltiplicativo degli elementi invertibili nell'anello $(\mathbb{Z}/8\mathbb{Z}, +, \cdot)$: ha cardinalitá 4, non é ciclico, é isomorfo al gruppo additivo prodotto diretto $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ detto **gruppo di Klein**; dedurre un isomorfismo di esso con il **gruppo delle simmetrie di un quadrato** o con il **sottogruppo** di $S_4 = Sym(4)$ formato dalle permutazioni

$$U(\mathbb{Z}/8\mathbb{Z}) \simeq \{Id_{S_4},\ (1,4)(2,3),\ (1,2)(3,4),\ (1,3),(2,4)\}.$$

Infine $U(\mathbb{Z}/8\mathbb{Z})$ ammette come sottogruppi propri non banali tre sottogruppi ciclici di ordine (o cardinalitá) 2.

(ii) $U(\mathbb{Z}/9\mathbb{Z})$= gruppo moltiplicativo degli elementi invertibili nell'anello $(\mathbb{Z}/9\mathbb{Z}, +, \cdot)$: ha cardinalitá 6, é ciclico, é isomorfo al gruppo additivo $(\mathbb{Z}/6\mathbb{Z}, +)$ ed il Teorema di Lagrange **si inverte con unicitá e ciclicitá**, in altri termini per ogni divisore k di $6 = |U(\mathbb{Z}/9\mathbb{Z})|$ esiste ed é unico il sottogruppo $H_k < U(\mathbb{Z}/9\mathbb{Z})$ di cardinalitá $|H_k| = k$ ed inoltre ciascun H_k é sottogruppo ciclico.

(iii) $U(\mathbb{Z}/10\mathbb{Z})$= gruppo moltiplicativo degli elementi invertibili nell'anello $(\mathbb{Z}/10\mathbb{Z}, +, \cdot)$: ha cardinalitá 4, é ciclico, é isomorfo al gruppo additivo $(\mathbb{Z}/4\mathbb{Z}, +)$, quindi non é isomorfo al gruppo di Klein del punto (i), e come nel punto (ii) il Teorema di Lagrange **si inverte con unicitá e ciclicitá**, in altri termini esiste un unico sottogruppo $H_2 < U(\mathbb{Z}/10\mathbb{Z})$ di cardinalitá 2 (unico divisore proprio di $4 = |U(\mathbb{Z}/10\mathbb{Z})|$) che é sottogruppo ciclico.

Esercizio 7. (i) Sia dato il gruppo additivo $(\mathbb{Z}/12\mathbb{Z}, +)$. Determinare, a meno di isomorfismo, la struttura del **gruppo degli automorfismi di gruppo**

$$(Aut(\mathbb{Z}/12\mathbb{Z}, +), \circ),$$

dove l'operazione di gruppo $\circ$ é la composizione di automorfismi.

(ii) Stabilire se il il gruppo additivo $(\mathbb{Z}/12\mathbb{Z}, +)$ é isomorfo al gruppo moltiplicativo $U(\mathbb{Z}/13\mathbb{Z})$= gruppo moltiplicativo degli elementi invertibili nell'anello $(\mathbb{Z}/13\mathbb{Z}, +, \cdot)$. In caso di risposta affermativa determinare un isomorfismo esplicito fra essi.

(iii) Determinare, a meno di isomorfismo, tutti i **gruppi immagine omomorfa** del gruppo additivo $(\mathbb{Z}/12\mathbb{Z}, +)$.

(iv) Determinare, a meno di isomorfismo, tutti i **gruppi immagine omomorfa** del gruppo moltiplicativo $U(\mathbb{Z}/12\mathbb{Z})$= gruppo moltiplicativo degli elementi invertibili nell'anello $(\mathbb{Z}/12\mathbb{Z}, +, \cdot)$